Commonwealth of Massachusetts
OFFICE OF THE COMPTROLLER
One Ashburton Place, 9th Floor
Boston, Massachusetts 02108
(617) 727-5000
MACOMPTROLLER.ORG

William McNamara
Comptroller

FOUR STEPS TO PREPARE FOR A CYBERSECURITY RISK ASSESSMENT

Entities deploy a wide array of information technology devices, systems, and applications across a wide geographic area. While these physical assets can be labeled and tracked using bar codes and databases, understanding and controlling the cybersecurity resilience of those systems and applications is a much larger challenge. Not being able to track the location and configuration of networked devices and software can leave an organization vulnerable to security threats that can cripple operations.

To assist entities with cyber readiness, the Office of the Comptroller provides departments with resources (see CTR Cyber) to assist them with meeting their data management and cybersecurity internal control requirements.

A **cybersecurity risk assessment** helps to identify security vulnerabilities and effectively mitigate risks, and the best way to prepare for this risk assessment is to have a detailed, current and accurate data security landscape. Simply:

- What data is collected, and where and how is the data collected and managed?
- Who has access to the data and how is access to the data is restricted?
- What data is essential to be protected (PII, confidential, system, client etc.)?
- Where are cybersecurity vulnerabilities?

The following four steps will help prepare an entity to perform a cybersecurity risk assessment that identifies and mitigates security risks. Entities can access a sample Cybersecurity Risk Assessment Inventory to help identifythe types of information needed for a cybersecurity risk assessment.

1) **Inventory data security requirements** of all statutes, standards, regulations, policies and procedures that apply to your entity related to the security, privacy and data retention and disposal of data collected, processed, transmitted and maintained by the entity. Some standard data and security policies include acceptable use, access and asset management, business continuity, disaster recovery and incident response, network security, logging, and event monitoring, physical security, vulnerability, and third-party requirements. See the Commonwealth's EOTSS Enterprise Security Policies and Standards.

2) **Inventory all data** collected, created, processed, transmitted and maintained by the entity. Data Inventory should classify data based upon privacy and security requirements (personally identifiable information (PII), confidential, sensitive, security, public, etc.) and data retention and disposal requirements. This inventory will be more effective if an entity identifies all the in-points of how the data is collected, who has access to the data, whether there are restrictions on access and the retention periods for the data (if applicable).

3) **Inventory all equipment and infrastructure** for all mediums throughout the entity that manage the data identified in the **Data Inventory**. Equipment and infrastructure include all PCs, servers, hardware, software, operating systems, networks, third party applications, Wi-Fi, data repositories (directories, PST, network, cloud), cell, tablets,BYOD, cabling and wiring, switches, modems and any other medium that creates, collects, stores or transmits entitydata. Entities can start with their current asset inventories and then add security related details.

4) **Create data maps or network diagrams** that show how the data identified in the **Data Inventory** flows throughout entity: data in-flows, data at rest, data archived, data in-transit and data outflows externally as listed in the **Equipment and Infrastructure Inventory**. The network traffic diagrams should also identify all the physical and virtual security controls that are in place at **each** in-point, exit-point, perimeter, etc. for each asset in the inventory. Physical and virtual security includes badge or key codes locks, alarms, security cameras, protections from physical damages (fire, water, electrical surges etc.), administrative access rights, segmentation, virus and malware protections, multi-factor authentication, logging and event monitoring, DMZ, firewalls, etc. used to protect data and assets from unauthorized access or physical damages.